

1 PIERCE O'DONNELL (SBN 081298)  
2 PODonnell@ggfirm.com  
3 TIMOTHY J. TOOHEY (SBN 140117)  
4 TToohey@ggfirm.com  
5 PAUL A. BLECHNER (SBN 159514)  
6 PBlechner@ggfirm.com  
7 GREENBERG GLUSKER FIELDS  
8 CLAMAN & MACHTINGER LLP  
9 2049 Century Park East, Suite 2600  
10 Los Angeles, California 90067  
11 Telephone: 310.553.3610  
12 Fax: 310.553.0687

13 Attorneys for Plaintiff  
14 MICHAEL TERPIN

15  
16 UNITED STATES DISTRICT COURT  
17 CENTRAL DISTRICT OF CALIFORNIA  
18 WESTERN DIVISION

19 MICHAEL TERPIN,  
20 Plaintiff,  
21 v.  
22 AT&T MOBILITY, LLC; and  
23 DOES 1-25,  
24 Defendants.

25 Case No. 2:18-cv-06975-ODW-KS  
26 [Assigned to The Hon. Otis D. Wright II]

27 **OPPOSITION OF PLAINTIFF  
28 MICHAEL TERPIN TO MOTION  
FOR SUMMARY JUDGMENT**

29 Hearing Date: March 27, 2023  
30 Time: 1:30 p.m.  
31 Trial: May 2, 2023

32 **[FILED UNDER SEAL PURSUANT TO  
33 COURT'S FEBRUARY 23, 2023  
34 ORDER [DKT 215]]**

35 GREENBERG GLUSKER FIELDS CLAMAN  
36 & MACHTINGER LLP  
37 2049 Century Park East, Suite 2600  
38 Los Angeles, California 90067

## 1 2 3 4 **TABLE OF CONTENTS**

		<b>Page</b>
5	I. INTRODUCTION.....	1
6	II. STATEMENT OF FACTS.....	3
7	A. The June 2017 SIM Swap .....	3
8	B. Harm to AT&T Customers from Increased SIM Swap Activity Was Foreseeable .....	4
9	C. Smith's December 2017 Unauthorized SIM Swaps .....	7
10	D. The January SIM Swap .....	8
11	III. LEGAL STANDARD .....	9
12	IV. ARGUMENT .....	10
13	A. The Economic Loss Doctrine Does Not Bar Terpin's Negligence Claims .....	10
14	B. The January SIM Swap Establishes A Valid Claim Under the FCA .....	12
15	1. The January SIM Swap Violated 47 U.S.C .....	12
16	2. "Exceeds Authorized Access" in the FCA does not have the same meaning as it does in the CFAA.....	14
17	C. Terpin's Breach of Contract Damages Are Proper and AT&T Cannot Exculpate Itself from Its Gross Negligence and Statutory Violations .....	16
18	D. Terpin Can Establish Proximate Cause .....	18
19	V. CONCLUSION .....	23
20		
21		
22		
23		
24		
25		
26		
27		
28		

**GREENBERG GLUSKER FIELDS CLAMAN**  
**& MACHTINGER LLP**  
 2049 Century Park East, Suite 2600  
 Los Angeles, California 90067

## TABLE OF AUTHORITIES

	Page
1 <b>CASES</b>	
5 <i>Biakanja v. Irving</i> , 49 Cal.2d 647 (1958) .....	10
7 <i>California v. Superior Court</i> , 150 Cal.App.3d 848 (1984).....	20
8 <i>Circuit City Stores, Inc. v. Adams</i> , 279 F.3d 889 (9th Cir. 2002).....	3, 11
9 <i>Desrosiers v. Flight Int'l</i> , 156 F.3d 952 (9th Cir. 1988).....	18
11 <i>Dutch Enterprises, Inc. v. Consolidated Freightways</i> , 1993 WL 266702 (N.D.Cal. 1993).....	17
13 <i>Food Safety Net Services v. Eco Safe Systems USA, Inc.</i> , 209 Cal.App.4th 1118 (2012).....	3
14 <i>Fraser v. Mint Mobile, LLC</i> , 2022 WL 1240864 (N.D.Cal. 2022).....	22
16 <i>Greene v. Sprint Communications Co.</i> , 340 F.2d 1047 (9th Cir. 2003).....	14
17 <i>In the Matter of Cox Communications, Inc.</i> , 30 FCC Rcd. 12302 (2015) .....	13
19 <i>J'Aire Corp. v. Gregory</i> , 24 Cal.3d 799 (1979) .....	10
20 <i>Kumaraperu v. Feldsted</i> , 237 Cal.App.4th 60 (2015).....	18
22 <i>Li v. Yellow Cab Co.</i> , 13 Cal.3d 804 (1975) .....	23
23 <i>Matysik v. County of Santa Clara</i> , 2018 WL 72724 (N.D.Cal. 2018).....	3, 19
25 <i>Modisette v. Apple Inc.</i> , 30 Cal.App.5th 136 (2018).....	22
26 <i>Moore v. Centrelake Med. Group, Inc.</i> , 83 Cal.App.5th 515 (2022).....	12

1                   **TABLE OF AUTHORITIES**  
 2                   (continued)

	Page
4 <i>Osborn v. Irwin Memorial Blood Bank,</i> supra, 5 Cal.App.4th 234 (1992).....	18
5 <i>Paige v. New Haven Unified School Dist.,</i> 2010 WL 5396062 (N.D.Cal. 2010).....	19
7 <i>Sheen v. Wells Fargo, N.A.,</i> 12 Cal.5th 905 (2022) .....	2, 10, 11, 12
8 <i>Shih v. Starbucks Corp.,</i> 53 Cal.App.5th 1063 (2020).....	20, 21
10 <i>Steinle v. United States,</i> 17 F.4th 819 (9th Cir. 2021).....	21
11 <i>Sun-Maid Raisin Growers v. Victor Packing Co.,</i> 146 Cal.App.3d 787 (1983).....	17
13 <i>U.S. West, Inc. v. FCC,</i> 183 F.3d 1224 (10th Cir. 1999).....	14
15 <i>Van Buren v. United States,</i> 141 S.Ct. 1648 (2021) .....	15
16 <i>Wawanese Mut. Ins. Co. v. Matlock,</i> 60 Cal.App.4th 583 (1997).....	20, 21
17 <i>Whiteway v. FedEx Kinko's Office and Print Services,</i> 319 Fed. Appx. 688 (9th Cir. 2009).....	9, 10
19 <i>Williams v. Fremont Corners, Inc.,</i> 37 Cal.App.5th 654 (2019).....	19
21 <b>STATUTES</b>	
22                 47 U.S.C. § 222 .....	passim
23                 47 U.S.C. § 222(a) .....	12, 13, 14
24                 47 U.S.C. § 222(h)(1).....	13
25                 Computer Fraud and Abuse Act 18 U.S.C. § 1030 <i>et seq.</i> .....	15
26                 Federal Communications Act.....	passim
27	
28	

1                           **TABLE OF AUTHORITIES**  
2                           (continued)

3                           **Page**

4                           **OTHER AUTHORITIES**

5                          47 CFR § 64.2001 <i>et seq.</i> .....	11
6                          1 Witkin, <i>Summary of Cal. Law</i> (11th ed. 2022), Contracts, § 679 .....	17

7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

GREENBERG GLUSKER FIELDS CLAMAN  
& MACHTINGER LLP  
2049 Century Park East, Suite 2600  
Los Angeles, California 90067

## I. INTRODUCTION

Defendant AT&T Mobility, LLC’s (“AT&T”) motion for summary judgment (the “Motion”) should be denied due to the massive number of disputed material facts. In many ways, this motion is a thinly disguised rehash of AT&T’s prior unsuccessful motions to dismiss predicated on mischaracterizations of controlling law. As demonstrated below, it should meet the same fate.

AT&T's top executives recognize that customers count on AT&T and promised: “[t]hat we will follow not only the letter of the law, but the spirit of the law” and “will always take responsibility.” PF-23.<sup>1</sup> AT&T has failed to follow the letter of the law, and its contentious and technical defenses make a mockery of any attempt to follow the spirit of the law.

As a common carrier, AT&T is entrusted under the Federal Communications Act (“FCA”) with the duty of protecting its customers’ personal communications. *See* 47 U.S.C. § 222. Yet, AT&T allowed an authorized retailer employee (who had processed prior unauthorized SIM swaps that AT&T failed to investigate) to bypass AT&T’s own security procedures, including the “extra security” that AT&T had urged Plaintiff Michael Terpin (“Terpin”) to put on his account to prevent unauthorized SIM swaps. That unauthorized SIM swap resulted in Terpin’s loss of almost \$24 million in cryptocurrency.

AT&T seeks to revive in this motion (the “Motion”) many of the arguments denied in its motions to dismiss this case. AT&T ignores the mountain of evidence that it knew that unauthorized SIM swaps were exposing customer’s personal communications and causing financial losses to its customers. AT&T also engages in a classic “blame the victim” defense, seeking to turn Plaintiff’s alleged comparative fault into a complete defense, while brazenly defending AT&T’s gross negligence in allowing an employee with a prior history of unauthorized SIM swaps

---

<sup>1</sup> The format “PF-##” refers to the additional “Plaintiff’s Facts”, as numbered, in Section II of Plaintiff’s Statement of Genuine Disputes of Material Facts.

1 to hand control over Terpin’s phone to Ellis Pinsky, who has admitted his lead role  
 2 in the SIM swap and theft.

3 The facts presented by Terpin and the proper inferences drawn from them,  
 4 prevent entry of summary judgment in this case.

5 *First*, the economic loss doctrine (rejected by the Court in AT&T’s second  
 6 motion to dismiss) is inapplicable here. AT&T’s reliance on *Sheen v. Wells Fargo*,  
 7 N.A., 12 Cal.5th 905 (2022) (“*Sheen*”), is misplaced. As reinforced by *Sheen*, the  
 8 economic loss doctrine does not apply where a duty arises outside the bounds of the  
 9 negotiated contract. Here, AT&T had duties to protect customers’ communications  
 10 and implement an information security program under (a) the FCA and other  
 11 statutory law and (b) a 2015 Consent Decree from the Federal Communications  
 12 Commission (FCC). These duties arise separately from the contract of adhesion  
 13 (also known as the wireless customer agreement (“WCA”)) between Terpin and  
 14 AT&T.

15 *Second*, in another argument rejected previously by the Court, Terpin has  
 16 demonstrated valid FCA claims. AT&T exposed Terpin’s personal and proprietary  
 17 information by turning over control of the phone to unauthorized third parties,  
 18 allowing them to receive password reset messages while controlling Terpin’s phone  
 19 number, to use Terpin’s phone as a means of authentication to impersonate him,  
 20 and to access files in his online accounts. As the FCC has recognized, not only  
 21 does the FCA protect more than technical aspects of Customer Proprietary  
 22 Information (“CPNI”), but an unauthorized SIM swap allows the perpetrator to gain  
 23 control (and misuse) a customer’s CPNI.

24 AT&T’s alternate reliance on a criminal federal statute with a different  
 25 purpose (i.e., the Computer Fraud and Abuse Act (CFAA)) is frivolous and  
 26 unsupported by any authority. AT&T’s proffered interpretation of Section 222  
 27 would unjustifiably exempt AT&T from liability where AT&T had notice that an  
 28

1 employee had previously accessed customer accounts and had failed to prevent  
 2 repeat occurrences of such misconduct.

3       *Third*, Terpin’s contract claims are viable. AT&T cannot insulate itself  
 4 through a limitation of liability clause resulting from “unequal bargaining power or  
 5 [that is] contrary to public policy.” *Food Safety Net Services v. Eco Safe Systems*  
 6 *USA, Inc.*, 209 Cal.App.4th 1118, 1126 (2012). The WCA is a classic contract of  
 7 adhesion that attempts to exculpate AT&T from almost all liability. *Circuit City*  
 8 *Stores, Inc. v. Adams*, 279 F.3d 889, 893 (9th Cir. 2002) (contract of adhesion is  
 9 “standard form contract, drafted by the party with superior bargaining power which  
 10 relegates to the other party the option of either adhering to its terms without  
 11 modification or rejecting the contract entirely”). Separate from the WCA, AT&T  
 12 promised Terpin “extra security” after his first unauthorized SIM swap in June  
 13 2017 to protect him against a reoccurrence. Such breached promises outside the  
 14 WCA (consistent with its security and privacy commitments) are not subject to any  
 15 purported limitation of liability.

16       *Finally*, AT&T has concocted a spurious version of the events leading to the  
 17 January 2018 theft that misleadingly omits AT&T’s role and ignores the  
 18 foreseeability of what occurred. The theft immediately after the January 7, 2018  
 19 unauthorized SIM swap was not remote or attenuated, but rather exactly what the  
 20 perpetrator hoped and what he and others had done on prior occasions. Material  
 21 facts regarding the foreseeability of Terpin’s injury render causation inappropriate  
 22 for summary judgment in AT&T’s favor. *See Matysik v. County of Santa Clara*,  
 23 2018 WL 72724 \*14 (N.D.Cal. 2018) (“if reasonable persons could differ over the  
 24 question of foreseeability, … the question should be left to the jury”).

25 **II. STATEMENT OF FACTS**

26       A. The June 2017 SIM Swap

27       On June 11, 2017, Terpin suffered an unauthorized SIM swap on his account  
 28 (“June 2017 SIM Swap”). *See* PF-26-28. [REDACTED]

1

[REDACTED]

2 PF-27. Terpin promptly complained of fraud to AT&T, including  
 3 informing AT&T that his Skype (Microsoft) account had been compromised and  
 4 that he had lost cryptocurrency in the June 2017 SIM Swap. PF-29-30,32-33.

5 When Terpin met with AT&T representatives on June 13, 2007, they offered  
 6 him “celebrity” or “extra” security, i.e., an upgrade from a four-digit to a six-digit  
 7 code that he was told could not be changed by anyone other than himself  
 8 (hereinafter, “extra security”). PF-33-44. AT&T promised that the “extra security”  
 9 would be needed to make account changes, including swapping a SIM to another  
 10 phone. PF-35. AT&T supposedly placed the “extra security” on Terpin’s account,  
 11 adding a “special instruction” displayed in Terpin’s account in red that AT&T was  
 12 not to validate Terpin unless he came into a store. PF-36-37.

13

[REDACTED]

14 PF-38,40. Terpin believed AT&T’s promises that his  
 15 account would be protected against future unauthorized SIM swaps because of the  
 16 “extra security” and Terpin remained an AT&T customer. PF-39,41-43. AT&T’s  
 17 promise was standard practice and consistent with AT&T’s September 27, 2017  
 18 Cyber Aware blog post to customers (“Cyber Aware Blog”) that the best way to  
 19 protect themselves against unauthorized SIM swaps was placing “extra security” on  
 20 their accounts. PF-44.

21

B. Harm to AT&T Customers from Increased SIM Swap Activity Was  
 Foreseeable.

23 AT&T did not disclose to Terpin when making the June 2017 assurances or  
 24 in its September 27, 2017 customer notice that the added “extra security” was an  
 25 ineffective security measure, [REDACTED]  
 26 [REDACTED]  
 27 [REDACTED]  
 28 [REDACTED]

GREENBERG GLUSKER FIELDS CLAMAN  
 & MACHTINGER LLP  
 2049 Century Park East, Suite 2600  
 Los Angeles, California 90067

1 [REDACTED]  
 2 [REDACTED]  
 3 [REDACTED]  
 4 [REDACTED] PF-46-47.  
 5 [REDACTED]<sup>2</sup>  
 6 [REDACTED] PF-48.  
 7 [REDACTED]  
 8 [REDACTED]  
 9 [REDACTED] PF-49. See also PF-62-64.  
 10 [REDACTED]  
 11 [REDACTED]  
 12 [REDACTED]  
 13 [REDACTED] PF-65-68.  
 14 [REDACTED]  
 15 [REDACTED]  
 16 [REDACTED]

17 PF-70.

18 Well before the January 2018 SIM Swap, AT&T knew or should have known  
 19 that unauthorized SIM swaps were targeting cryptocurrency holders because such  
 20 thefts were irreversible. Indeed, AT&T was obligated to track such emerging fraud  
 21 by a 2015 Consent Decree with the FCC, which required AT&T to pay a \$25  
 22 million fine and implement an “Information Security Program” to both “identify  
 23 and respond to emerging risks or threats” to its customers’ privacy. PF-8-14.

24 \_\_\_\_\_  
 25 <sup>2</sup> “Authorized retailers” are third party vendors with exclusive agreements to sell  
 26 AT&T services and equipment. PF-87. Two examples of ARs are Spring  
 27 Communications (“Spring”), whose employee performed the January 2018 SIM  
 28 Swap, and Prime Communications (“Prime”) who was Spring’s successor. PF-88.  
 AR employees use AT&T’s systems (like OPUS), display AT&T logos, sell only  
 AT&T products and are indistinguishable from AT&T owned and operated stores.  
 PF-90-92. AR employees are supposedly required to follow AT&T procedures in  
 authenticating customers. PF-92.

1           AT&T also must have known that regulatory agencies had warned against  
 2 unauthorized SIM swaps (GDMP-50-52) and that a December 12, 2016 *Forbes*  
 3 article highlighted that SIM swaps led to thefts of cryptocurrency from customers  
 4 and that “telcos” were being blamed for not safekeeping their customers’ telephone  
 5 numbers. PF-53-56. *See also* August 21, 2017 *New York Times* and September 28,  
 6 2017 jdsupra.com articles, highlighting thefts of cryptocurrency through SIM  
 7 swaps, including those involving AT&T. PF-57-60. [REDACTED]

8 [REDACTED]  
 9 [REDACTED] PF-61.

10           On September 27, 2017, AT&T’s Cyber Aware Blog warned its customers  
 11 about what they should know about “SIM Swap Scams.” PF-73. The article  
 12 detailed how a “thief” will convince a service provider to replace a victim’s SIM  
 13 which will have the effect of “the mobile network . . . sending calls and texts to the  
 14 new SIM card—which is really the thief’s phone,” after which the victim’s phone is  
 15 deactivated and “the thief may be able to gain access to your financial or social  
 16 media accounts.” PF-74-75. The article warned that this “could happen to  
 17 anyone.” PF-76. AT&T’s chief recommendation to customers was to add “extra  
 18 security” to their accounts—a PIN that the customer must provide “before any  
 19 significant changes can be made.” PF-77.

20           The problem of unauthorized SIM swaps [REDACTED]  
 21 [REDACTED] exacerbated both by the proliferation of personal information to the  
 22 dark web (such as SSNs) caused by the 2017 Equifax breach (which could be used  
 23 by perpetrators of fraud) and the rise of cryptocurrency. PF-72,78-81. Indeed, in  
 24 2017, cryptocurrency had “joined the global financial system” and had a market  
 25 capitalization of \$100.1 billion dollars. PF-80-81. And, consistent with what  
 26 AT&T was seeing and what was being publicly reported, the chief perpetrator of  
 27 the January 2018 SIM Swap—Ellis Pinsky (“Pinsky”)—became aware of and  
 28 began SIM swapping for the purpose of stealing cryptocurrency in 2017. PF-82-85.

1           C.     Smith's December 2017 Unauthorized SIM Swaps.

2           Foreshadowing what would occur during the January 2018 SIM Swap,  
 3 Jahmil Smith ("Smith"), a Spring employee at an AT&T branded store in Norwich,  
 4 Connecticut, conducted two unauthorized SIM swaps on December 9, 2017 (the  
 5 "Prior Smith SIM Swaps"). PF-93-118.  
 6 [REDACTED]

7 [REDACTED] PF-94. Under AT&T's policies, this should have  
 8 triggered an investigation by AT&T's fraud or asset protection departments. PF-  
 9 95. Yet, AT&T either failed to review the account notes showing that these were  
 10 fraudulent or did not understand their import, labeling one a "technical" issue and  
 11 leaving it to the customer to contact law enforcement or fraud, while AT&T itself  
 12 did not refer either of the Prior Smith SIM Swaps to fraud. PF99-107.  
 13 As a result, AT&T did not investigate the Prior Smith SIM Swaps. PF-105. Spring  
 14 was also not informed, precluding it from investigating as well. PF-108-111.

15           If the incidents had been referred and investigated, AT&T "wouldn't have  
 16 allowed [Smith's] access to [AT&T's] system to remain." PF-98,106-107. Yet,  
 17 Smith was simply allowed to continue to work in AT&T's Norwich store by  
 18 himself without other employees or supervisors including during and after the  
 19 January 2018 SIM Swap. PF-113-115.

20           A few weeks after the Prior Smith SIM Swaps, a Norwich Police  
 21 Department report reveals that Smith reported a robbery in the AT&T branded store  
 22 when he was working alone on January 1, 2018, with the Spring regional manager  
 23 detailing the cash and inventory losses. PF-119-127. On the same day, that  
 24 manager told police that he believed Smith was involved and the robbery was an  
 25 "inside job." PF-124. The detectives also questioned Smith's truthfulness, and  
 26 Smith subsequently acknowledged his involvement, was arrested and charged, and  
 27 made restitution payments to AT&T in 2021. PF-127-130.

1           Where AT&T did not inform Spring about the Prior Smith SIM Swaps,  
2 Spring did not inform AT&T about the January 1, 2018 robbery. PF-131.  
3 Apparently, neither was obligated to inform the other of likely employee  
4 misconduct. PF-116-118.

5           Despite the Prior Smith SIM Swaps and despite Spring's immediately  
6 stated concerns about Smith's involvement in the January 1, 2018 robbery, AT&T  
7 did not revoke Smith's access to its computer system, Spring imposed no  
8 restrictions on Smith, and Smith continued to process SIM swaps in the days that  
9 followed, including processing the January SIM Swap. PF-132-133,114-115.

10           D.     The January SIM Swap

11 [REDACTED]

12 [REDACTED] PF-134-140,154-158.

13 Smith used AT&T's OPUS system to conduct the SIM swap. PF-136. [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 [REDACTED]

18 [REDACTED]

19 [REDACTED] PF-137-139. The transferred SIM was immediately active

20 and was controlled by Pinsky's "holder" [REDACTED]

21 [REDACTED] PF-140-141,153,159.

22           After the SIM swap, Terpin's wife, Maxine Hopkinson, attempted repeatedly  
23 to get AT&T to reverse the SIM swap and transfer the number back to Terpin's  
24 device. She was transferred to AT&T's fraud department, which twice did not pick  
25 up her calls. PF-142-145. Incredibly, even though Terpin's account was  
26 previously noted for fraud and Ms. Hopkinson complained about "fraud issues,"  
27 PF-143-150, AT&T never investigated the January 2018 SIM Swap. PF-151-152.

1       Shortly after the SIM for Terpin's account was transferred to Pinsky's  
2 "holder," the perpetrators changed the password for Terpin's Microsoft account.  
3 PF-168. This password reset via the January 2018 SIM Swap allowed the  
4 perpetrators to access Terpin's Microsoft account and find a file which allowed  
5 them to steal the cryptocurrency. PF-162-166. [REDACTED]  
6 [REDACTED] PF-153.

7       Pinsky confirmed the details of the January 2018 SIM Swap and that he and  
8 others performed the SIM swap and theft. PF-154-172. A critical step in the SIM  
9 swap was Pinsky contacting Smith, who received a payment of between \$100 and  
10 \$500. PF-156-158. After the SIM swap occurred, Pinsky's "holder" controlled  
11 Terpin's phone and received the password reset text messages needed to reset  
12 Terpin's passwords. PF-159-160. Having obtained access to Terpin's accounts,  
13 Pinsky searched and eventually found a file in the trash of Terpin's Microsoft  
14 online account to access Terpin's cryptocurrency accounts. PF-161-163. Pinsky  
15 used this information to steal cryptocurrency then worth roughly \$24 million. PF-  
16 164.

17       Pinsky testified that he would not have been able to access Terpin's  
18 cryptocurrency accounts without the January 2018 SIM Swap because he had no  
19 way to access Terpin's Microsoft accounts. PF-165-166. Even so the January 2018  
20 Terpin SIM swap was one of the longest searches in which Pinsky was involved.  
21 PF-167.

22 **III. LEGAL STANDARD**

23       "To succeed on a motion for summary judgment, the movant must first  
24 demonstrate 'that there is no genuine issue as to any material fact and that the  
25 movant is entitled to judgment as a matter of law.'" *Whiteway v. FedEx Kinko's*  
26 *Office and Print Services*, 319 Fed. Appx. 688 (9th Cir. 2009), quoting  
27 Fed.R.Civ.P. 56(c). To defeat a showing by the movant, "the nonmovant must go  
28 beyond the pleadings to designate specific facts showing a genuine issue for

1 trial.” *Id.* “An issue is genuine ‘if the evidence is such that a reasonable jury could  
 2 return a verdict for the non-moving party.’” *Id.*, quoting *Anderson v. Liberty*  
 3 *Lobby, Inc.*, 477 U.S. 242, 248 (1986). “In conducting the summary judgment  
 4 analysis, all justifiable inferences are to be drawn in the non-moving party’s favor.”  
 5 *Id, citing Anderson* at 255.

6 **IV. ARGUMENT**

7       A.     The Economic Loss Doctrine Does Not Bar Terpin’s Negligence  
 8 Claims.

9              The Court previously rejected AT&T’s attempt to raise the economic loss  
 10 doctrine to dismiss Terpin’s complaint, finding that Terpin adequately alleged a  
 11 “special relationship” under *J’Aire Corp. v. Gregory*, 24 Cal.3d 799, 804 (1979)  
 12 and *Biakanja v. Irving*, 49 Cal.2d 647, 650 (1958). *See Dkt. 37 at 9.*

13              AT&T’s renewed economic loss doctrine argument seeks to dismiss Terpin’s  
 14 negligence claims (Claims 3-5) based on the recently decided California Supreme  
 15 Court case of *Sheen*. AT&T’s reliance on *Sheen* erroneously focuses solely on the  
 16 “privity” issue *without recognizing AT&T’s non-contractual duties*. However,  
 17 *Sheen* was limited to situations where “the litigants are in contractual privity **and**  
 18 the plaintiff’s claim is not ‘independent of the contract arising from principles of  
 19 tort law.’” 12 Cal.5th at 942 (emphasis added).

20              The *Sheen* case involved a borrower’s negligence claim alleging a “special  
 21 relationship” with a lender in the context of a loan modification application. The  
 22 California Supreme Court expressly concluded that there were no state or federal  
 23 statutory or regulatory duties at issue. *Id.* at 921.

24              By contrast, AT&T has a statutory obligation under the FCA to preserve the  
 25 privacy of customers’ calls. *See 47 U.S.C. § 222 and discussion re FCA, infra.*  
 26 AT&T also had an obligation under a 2015 consent decree (under which AT&T  
 27 was fined \$25 million) to implement an information security program, including

1 monitoring for emerging threats to customers' personal and proprietary  
 2 information. *See GDFM-8,10.*

3 Unlike *Sheen*, where the plaintiff could "not identify any statute or regulation  
 4 that requires Wells Fargo to treat his modification applications with due care," 12  
 5 Cal.5th at 920, Terpin *has identified statutory authority, regulations and orders*  
 6 requiring AT&T, as a common carrier, to protect the privacy of his communications  
 7 and guard against emerging threats, such as unauthorized SIM swaps leading to  
 8 customers' financial losses. *See, e.g.*, 47 U.S.C. § 222 (duty of common carrier to  
 9 protect privacy); 47 CFR § 64.2001 *et seq.* (FCC CPNI Rules); 2015 Consent  
 10 Decree at ¶ 18(b)-(c). Moreover, this statutory and regulatory authority, and the  
 11 FCC Consent Decree, are all directly on point (unlike in *Sheen* where the court  
 12 found there was nothing in the "extensive body of state and federal legislation and  
 13 regulations that address mortgage servicing" or in common law that created a duty  
 14 of the lender to the borrower regarding loan modifications). 12 Cal.5th at 921-22.

15 AT&T's economic loss doctrine argument alternatively fails because:

- 16 • Unlike *Sheen*, which involved a commercially negotiated loan contract  
     between the parties, the WCA is a classic contract of adhesion and Terpin  
     had no opportunity to negotiate its terms. *Id.* at 922-24. *See, e.g., Circuit*  
     17 *City Stores, Inc.*, 279 F.3d at 893 (contract of adhesion not subject to  
     negotiation by customer).
- 18 • Where *Sheen* asserted a "duty that is contrary to the rights and obligations  
     clearly expressed in the loan contract," AT&T's duty to protect the  
     privacy of Terpin's communications is complementary to the WCA.<sup>3</sup>  
     19 AT&T's privacy policy is incorporated by reference into the WCA and  
     states that AT&T has "implemented technology and security features and  
     20

---

21     22     23     24     25     26  
 27     <sup>3</sup> While AT&T's duties under the WCA to Terpin and all of its customers are  
 28     complementary to the duties under the FCA and the Consent Order, AT&T is not,  
     by contract, able to modify its statutory and other legal duties.

strict policy guidelines to safeguard the privacy of [customers'] Personal Information." *See* Exh. 18.

- *Sheen* also recognized another applicable exception to the economic loss rule for consumer contracts for professional services where professionals agree to undertake careful efforts to render services. In such cases, "most clients do not know enough to protect themselves by inspecting the professional's work or by other independent means." 12 Cal.5th at 933 (quoting *Restatement 3d. Torts*, Liability for Economic Harm sec. 4, com. A., p. 22). A consumer of mobile telephone services similarly does not have the technical expertise regarding security and authentication procedures to know how to protect herself from security and privacy.<sup>4</sup>

**B. The January SIM Swap Establishes A Valid Claim Under the FCA.**

1. The January SIM Swap Violated 47 U.S.C. § 222(a).

AT&T misconstrues Terpin's FCA claim by arguing that there was no exposure of CPNI through the January 2018 SIM swap, even though the perpetrators gained complete control over Terpin's phone, communications, and account. AT&T's argument is not only factually inaccurate (the perpetrators of the SIM swap indeed gained control of Terpin's CPNI and other private and proprietary information), but also fundamentally misconstrues Terpin's claim which is much broader and relates to the exposure of personal and proprietary information, in addition to CPNI.

CPNI is only a subset of information protected by Section 222 of the FCA, which also imposes a duty to protect the "confidentiality of proprietary information." *See* 47 U.S.C. § 222(a);

---

<sup>4</sup> *Moore v. Centrelake Med. Group, Inc.*, 83 Cal.App.5th 515 (2022), which AT&T cites, is equally unpersuasive. In *Moore*, the court affirmed dismissal under the economic loss rule because, unlike here, plaintiff "failed to show their claim is independent of their contracts and could show no separate duty."

1       <https://www.fcc.gov/enforcement/areas/privacy> (“Section 222 restricts carriers’ use  
 2 and disclosure of their customers’ (and certain other entities’) “proprietary”  
 3 information and requires that telecommunications carriers protect the  
 4 confidentiality of that information.”) CPNI is defined as the “quantity, *technical*  
 5 *configuration*, type, *destination*, *location* and amount of use of a  
 6 telecommunications service subscribed to by any customer of a telecommunications  
 7 carrier and that is made available solely by virtue of the carrier-customer  
 8 relationship.” 47 U.S.C. § 222(h)(1) (emphasis added).

9           AT&T’s argument that no one gained access to Terpin’s CPNI exalts form  
 10 over substance and is contrary to the FCC’s interpretation of what happens in an  
 11 unauthorized SIM swap. Through the actions of Smith, who saw details of Terpin’s  
 12 account information while “authenticating” Terpin and processing the SIM swap,  
 13 the perpetrators of the unauthorized SIM swap were able to take over Terpin’s  
 14 telephone number through a SIM swap (*i.e.*, the “technical configuration” of his  
 15 account) and access communications (such as password reset messages) that were  
 16 meant for Terpin’s phone (*i.e.*, both “destination” and “location” information). *See*  
 17 PF-159-160,163,171-172. It is difficult to imagine a more egregious violation of  
 18 the privacy of a customer’s private and proprietary communications than turning  
 19 over a customer’s entire phone to unauthorized parties who are able (i) to intercept  
 20 the private calls and messages meant for the customer and (ii) to use the phone  
 21 account as a means of authentication to impersonate the customer.

22           The FCC has made clear that Section 222 protects not only the technical  
 23 aspects of CPNI (such as call details), but also proprietary and private customer  
 24 information. *See In the Matter of Cox Communications, Inc.*, 30 FCC Rcd. 12302,  
 25 12307 (2015) (Section 222(a) [applies] to customer ‘proprietary information’ that  
 26 *does not fit within the statutory definition of CPNI*) (emphasis added). The FCC’s  
 27 authoritative interpretation of the FCA is entitled to deference because “the FCC is  
 28 the agency that is primarily responsible for the interpretation and implementation of

1 the Telecommunications Act and its own regulations.” *Greene v. Sprint*  
 2 *Communications Co.*, 340 F.2d 1047, 1052 (9th Cir. 2003).

3 Moreover, the FCC in 2021 in proposing amendments to its regulations to  
 4 better guard against SIM swaps did so on the basis that SIM swaps violate Section  
 5 222(a) and the regulations pertaining to that provision. *See* PF-15-18 (Notice of  
 6 Proposed Rulemaking (“NPR”)). In the NPR, the FCC proceeded under its  
 7 authority under Section 222 to provide regulations to prevent unauthorized SIM  
 8 swaps to “protect the confidentiality of proprietary information of and relating to  
 9 customers”. PF-16. In describing the mechanics of unauthorized SIM swaps, the  
 10 FCC also adopts what Terpin believes is the correct view that “the bad actor  
 11 [perpetrating a SIM swap] gains access to all of the information associated with the  
 12 customer’s account, including CPNI, and gains control over the customer’s phone  
 13 number and receives both text messages and phone calls intended for the victim”  
 14 thus violating section 222 of the FCA. PF-17 (emphasis added).

15 Disputed issues of fact prevent summary judgment for AT&T on this claim.  
 16 The confidential proprietary and personal information accessed from Terpin  
 17 includes classic CPNI such as Terpin’s SIM number, real-time confirmations of the  
 18 receipt of messages, the contents of messages and highly proprietary information  
 19 about his online accounts and cryptocurrency accounts. *See also U.S. West, Inc. v.*  
 20 *FCC*, 183 F.3d 1224, 1235 (10th Cir. 1999) (information protected by Section 222  
 21 is “extremely personal” to customers).

22 2. “Exceeds Authorized Access” in the FCA does not have the  
 23 same meaning as it does in the CFAA.

24 AT&T next asserts the patently faulty argument that it did not violate the  
 25 FCA because the term “exceeds authorized access” in the FCC regulations  
 26 pertaining to Section 222 should have the same meaning as the same phrase in the  
 27 Computer Fraud and Abuse Act (“CFAA”) 18 U.S.C. § 1030 *et seq.* as interpreted  
 28 by the Supreme Court in *Van Buren v. United States* to not criminalize “a

1 breathtaking amount of commonplace computer activity.” 141 S.Ct. 1648, 1652,  
 2 1661 (2021). This frivolous argument ignores that the FCA and CFAA are entirely  
 3 different statutes with different purposes and that the term “authorized” in the FCA  
 4 regulations has an entirely different meaning and applies to an entirely different set  
 5 of individuals than the CFAA.

6         Although it may make sense (as the *Van Buren* Court held) to restrict the  
 7 criminal penalties imposed by the CFAA to hackers (as opposed (for example) to  
 8 employees exceeding their authorized access to computer services), the provisions  
 9 relating to the regulation of common carriers under the FCA, including section 222,  
 10 are not a criminal statute that implicates ordinary computer users, but rather a  
 11 regulation applying only to “common carriers,” such as AT&T. Moreover, the  
 12 exemption that AT&T asks this Court to write into the statute would effectively  
 13 immunize AT&T from liability for failing to protect the private communications of  
 14 its customers by limiting the FCA in a way that is contrary to the FCC’s own  
 15 regulations and orders. It makes even less sense that any such exemption would  
 16 have ***no*** limitations and thereby permit carriers, like AT&T, to claim absolute  
 17 immunity notwithstanding the carrier’s *notice* of prior occasions where employees  
 18 acting within the AT&T system—such as Smith—had previously improperly  
 19 accessed accounts and AT&T knew that it had corrupt employees who were  
 20 bypassing proper authentication. There is no policy reason to allow AT&T to gut  
 21 Section 222 through such a convoluted argument.

22         C.     Terpin’s Breach of Contract Damages Are Proper and AT&T Cannot  
 23 Exculpate Itself from Its Gross Negligence and Statutory Violations.

24         Terpin’s breach of contract claim encompasses not only the WCA contract of  
 25 adhesion, but also AT&T’s promise to provide Terpin with “extra security” to  
 26 prevent what AT&T itself recognized were potentially serious financial losses to its  
 27 customer accounts. Terpin’s damages here were foreseeable both as the breach of  
 28 AT&T’s promises regarding security in the WCA, and the promises that it made to

1 Terpin (and other potential victims of an unauthorized SIM swaps) regarding extra  
 2 security.

3       Although AT&T cites *Lewis Jorge Constr. Mgmt.*, 34 Cal.4th 960 (2004)  
 4 regarding contract damages, it omits pertinent language. “Unlike general damages,  
 5 special damages are those losses that do not arise directly and inevitably from any  
 6 similar breach of any similar agreement. Instead, they are secondary or derivative  
 7 losses arising from circumstances that are particular to the contract or to the parties.  
 8 Special damages are recoverable if the special or particular circumstances from  
 9 which they arise were actually communicated to or known by the breaching party (a  
 10 subjective test) *or were matters of which the breaching party should have been*  
 11 *aware at the time of contracting (an objective test).*” 34 Cal.4th at 968-69 (citations  
 12 omitted) (emphasis added).

13       AT&T’s obligations under the WCA are ongoing and evolve as facts and  
 14 circumstances change. AT&T cannot legitimately claim that it had no obligation to  
 15 adjust its security to address emerging threats, particularly when the 2015 Consent  
 16 Decree requires that it does so. By September 27, 2017 or well before, AT&T had  
 17 actual knowledge that its customers were suffering substantial financial losses  
 18 because of unauthorized SIM swaps and recommended that the customers adopt  
 19 “extra security” to protect themselves against such losses. *See* PF-73-77. More  
 20 specifically, after Terpin’s first unauthorized SIM swap in June 2017 [REDACTED]  
 21 [REDACTED] Terpin was promised and received extra  
 22 security from AT&T, [REDACTED]  
 23 [REDACTED]

24 [REDACTED] PF-33-37.

25       More generally, the breaching party (AT&T) “should have been aware” at  
 26 the time that it promised Terpin extra security (i.e., June 2017) and certainly by the  
 27 time it breached its agreement to provide extra security that investors in  
 28 cryptocurrency were suffering financial losses. The failure to implement proper

1 security with such knowledge constitutes gross negligence and misrepresentation to  
 2 its customers. *See, supra*, section II.B.

3 The foreseeability of damages is a fact intensive inquiry. *Dutch Enterprises,*  
 4 *Inc. v. Consolidated Freightways*, 1993 WL 266702 \*2 (N.D.Cal. 1993); *Sun-Maid*  
 5 *Raisin Growers v. Victor Packing Co.*, 146 Cal.App.3d 787, 790 (1983)  
 6 (foreseeability of damages question for the trier of fact). In this case, AT&T argues  
 7 that it was not foreseeable in 1996 that Terpin would invest in cryptocurrency  
 8 (which hadn't been invented yet). But the WCA is not a "one and done"  
 9 agreement, but instead imposes ongoing responsibilities on AT&T as circumstances  
 10 change. AT&T's promises regarding security were not locked into place in 1996  
 11 like an insect caught in a piece of amber. As it recognized in its September 27,  
 12 2017 *Cyber Aware Blog* recommending "extra security" to guard against SIM  
 13 swaps, AT&T's overarching obligations to preserve privacy and security were not  
 14 limited to what it knew about Terpin in 1996 before the smartphone was even  
 15 invented.

16 AT&T's limitation of liability clause also cannot be used to exculpate itself  
 17 from gross negligence or statutory violations, including those under the FCA. *See* 1  
 18 Witkin, *Summary of Cal. Law* (11th ed. 2022), Contracts, § 679, ("[t]he present  
 19 view is that a contract exempting from liability for ordinary negligence is valid  
 20 where no public interest involved and no statute expressly prohibits it... But  
 21 there can be no exemption from liability for intentional wrong, gross negligence, or  
 22 violation of law") (*citing Haliday v. Greene*, 244 Cal.App.3d 482, 488 (1966)). In  
 23 any event, the only exculpatory provision at issue is in the WCA and AT&T, as  
 24 alleged above, engaged in gross negligence and misrepresentations to its customers,  
 25 particularly regarding the protection afforded by extra security against unauthorized  
 26 SIM swaps. There was no limitation of liability provision regarding the provision  
 27 of AT&T's extra security.

1        This argument fails for the reasons stated herein, and it clearly cannot be  
 2 reconciled with the promises of AT&T's highest-ranking executives that AT&T  
 3 will follow the spirit of the law and always take responsibility.

4        D. Terpin Can Establish Proximate Cause.

5        Proximate cause and causation in fact are generally questions "of fact for the  
 6 jury." *Desrosiers v. Flight Int'l*, 156 F.3d 952, 956 (9th Cir. 1988). The trier of  
 7 fact must determine whether the defendant has a duty to the plaintiff and whether  
 8 the harm that occurred to the plaintiff was foreseeable. *See Kumaraperu v.*  
 9 *Feldsted*, 237 Cal.App.4th 60, 69 (2015), citing *Cabral v. Ralphs Grocery Co.* 51  
 10 Cal.4th 764, 772, 779 (2011) ("the question of 'the closeness of the connection  
 11 between the defendant's conduct and the injury suffered' [citation] is strongly  
 12 related to the question of foreseeability itself." . . . . The court's task is to "evaluate  
 13 more generally whether the category of negligent conduct at issue is sufficiently  
 14 likely to result in the kind of harm experienced that liability may appropriately be  
 15 imposed.")

16        The jury's evaluation of causation is thus "a matter of probability and  
 17 common sense." *Osborn v. Irwin Memorial Blood Bank*, supra, 5 Cal.App.4th 234,  
 18 253 (1992). "If, as a matter of ordinary experience, a particular act or omission  
 19 might be expected to produce a particular result, and if that result has in fact  
 20 followed, the conclusion may be justified that the causal relation exists. In drawing  
 21 that conclusion, the triers of fact are permitted to draw upon ordinary human  
 22 experience as to the probabilities of the case." *Kumaraperu*, 237 Cal.App.4th at 69,  
 23 citing Rest.2d Torts, § 433B, com. b, p. 443. Moreover, foreseeability is not based  
 24 on the plaintiff's specific injury (theft of cryptocurrency) but rather on the general  
 25 character of the event or harm (financial losses from unauthorized SIM swaps).  
 26 *Williams v. Fremont Corners, Inc.*, 37 Cal.App.5th 654, 671 (2019).

27        AT&T ignores these fundamental principles of law.  
 28

1           The facts showing foreseeability are set forth in Section II.B. AT&T [REDACTED]  
 2 [REDACTED]

3 even warned its customers about such an eventuality on September 27, 2017.  
 4 AT&T knew—or should have known—that cryptocurrency had experienced  
 5 significant growth during 2017 and there are multiple public reports of SIM swaps  
 6 leading to crypto losses by mid-2017. Because AT&T was required under the 2015  
 7 Consent Decree to monitor emerging threats to its customers' privacy, AT&T  
 8 should be charged to have known about emerging threats described in the  
 9 widespread publicity regarding unauthorized SIM swaps involving cryptocurrency,  
 10 including in prominent articles from 2016-2017 in *Forbes*, the *New York Times* and  
 11 elsewhere.

12           There is nothing attenuated or remote about the cryptocurrency theft that  
 13 followed the January 7, 2018 Terpin SIM Swap—what happened is precisely what  
 14 Pinsky set out to do when he offered Smith the bribe to process this SIM swap on  
 15 AT&T's system and what AT&T itself predicted could happen to customers on  
 16 September 27, 2017. Grounded as this issue is in the fact intensive issue of the  
 17 foreseeability of harm, the issue of proximate causation is particularly inappropriate  
 18 for granting summary judgment in AT&T's favor. See *Matysik*, 2018 WL 72724 at  
 19 \*14 (“if reasonable persons could differ over the question of foreseeability,  
 20 summary judgment is inappropriate and the question should be left to the jury”);  
 21 *see also Paige v. New Haven Unified School Dist.*, 2010 WL 5396062 \*5 (N.D.Cal.  
 22 2010), *citing Hoyem v. Manhattan Beach City Sch. Dist.*, 22 Cal.3d 508, 520  
 23 (1978).

24           For purposes of defeating summary judgment, Terpin has shown a “natural  
 25 and continuous sequence” of plausible events connecting the hackers’ access to his  
 26 phone number through the January 7, 2018 SIM Swap to the theft of his  
 27 cryptocurrency. *California v. Superior Court*, 150 Cal.App.3d 848, 857 (1984).  
 28 Given the substantial evidence that substantiates the Complaint’s allegations on

1 these issues, it is unclear why AT&T would even attempt to raise this issue in the  
 2 Motion, particularly where the Court previously rejected AT&T's causation  
 3 argument. *See* Dkt. 37 at 5-7.

4       The cases cited by AT&T are readily distinguished and do not require a  
 5 different result on facts that present such a straightforward case of foreseeability.  
 6 Unlike the instant facts, where the theft of cryptocurrency after the SIM swap was  
 7 not only foreseeable, but was consistent with Pinsky's specific purpose and prior  
 8 activities PF-155,83-85, each of the cases relied on by AT&T involve factual  
 9 scenarios where the injury that followed the incident in question was either not  
 10 foreseeable at all, or at least not within the scope of the risk created by the  
 11 wrongdoing at issue.

12       In *Shih v. Starbucks Corp.*, 53 Cal.App.5th 1063 (2020), the plaintiff "spilled  
 13 her drink because after she walked to the table with the two hot drinks in her hands,  
 14 put her drink down, and removed the lid, she bent over the table, pushed out her  
 15 chair, lost her balance, grabbed the table to avoid falling, and knocked her drink off  
 16 the table." *Id.* at 1070. While the court concluded that losing one's balance while  
 17 seated or rising from the table may be foreseeable, it was not "within the scope of  
 18 the risk" created by the decision to serve a hot beverage without a protective sleeve.  
 19 *Id.* As the court explained, the failure to use the protective sleeve did not increase  
 20 the risk of the customer losing her balance. *Id.* Here, by contrast, AT&T's failures  
 21 increased the foreseeable risks to Terpin.

22       In *Wawanesa Mut. Ins. Co. v. Matlock*, 60 Cal.App.4th 583 (1997), the court  
 23 specifically found a lack of foreseeability when the purchase of cigarettes for a  
 24 minor led to the teasing of youngsters in the proximity of someone smoking that  
 25 allegedly caused the youngsters walking on telephone poles to get off those poles  
 26 and in the process bump into the person holding a cigarette, who then dropped the  
 27 cigarette which landed in an inaccessible and unrecoverable space between two  
 28 poles, which then resulted in a fire. *Id.* at 588-89. The court appropriately labeled

1 this unforeseeable string of events as the ‘‘Rube Goldbergesque system of fortuitous  
 2 linkages.’’ *Id.* at 588.

3 And, in *Steinle v. United States*, 17 F.4th 819 (9th Cir. 2021), the court used  
 4 that same description in a case where a loaded pistol was left in a vehicle, a person  
 5 broke into the locked vehicle and stole a seemingly innocuous backpack, the person  
 6 found a pistol in that backpack, removed the pistol from the holster and wrapped it  
 7 in a cloth before abandoning or losing it a half mile away, where another person  
 8 then found the pistol four days later and fired it, apparently aimlessly, and a bullet  
 9 then ricocheted off the ground and struck the victim. *Id.* at 822-23.

10 *Shih*, *Wawanesa*, and *Steinle* are based on the absence of foreseeability and  
 11 resulted from fact patterns that resulted in harm that the courts determined would  
 12 never have been predicted (and *Wawanesa* and *Steinle* involved third parties who  
 13 had no relationship with the plaintiff). By contrast, the harm suffered by Terpin  
 14 was the very financial harm that AT&T itself found was foreseeable (*see* September  
 15 27, 2017 Cyber Aware Blog) and that was described in numerous articles  
 16 describing cryptocurrency theft from unauthorized SIM swaps. While AT&T seeks  
 17 to dress up what occurred between the SIM swap and the theft to make it appear  
 18 more complicated, what happened following the January 2018 SIM Swap [REDACTED]

19 [REDACTED]  
 20 [REDACTED] PF-61.

21 Moreover, what happened is what the perpetrators hoped, i.e., using a SIM swap to  
 22 reset passwords to access accounts for the purpose of obtaining information needed  
 23 to access cryptocurrency wallets and to steal cryptocurrency. PF-155.

24 This sequence of events was direct, natural and continuous—not a series of  
 25 fortuitous linkages. *See, e.g., Fraser v. Mint Mobile, LLC*, 2022 WL 1240864  
 26 (N.D.Cal. 2022) (the allegations of proximate cause—in a SIM swap case resulting  
 27 in the draining of cryptocurrency just one hour, eleven minutes after the SIM  
 28 swap—“are sufficiently direct and not comparable to the ‘Rube Goldbergesque

1 system of fortuitous linkages' where California courts have held proximate cause  
 2 lacking as a matter of law").<sup>5</sup>

3 Moreover, in all of these cases, the facts that made the resulting harm too  
 4 attenuated all involved *subsequent/intervening* actions occurring *after* the  
 5 defendant's conduct. Here, by contrast, the extended attack that AT&T directs at  
 6 Terpin's security practices and how his cryptocurrency keys ended up in the  
 7 Microsoft account that Pinsky accessed by virtue of the unauthorized SIM swap had  
 8 already occurred *before* the January 2018 SIM Swap. AT&T cites no actions taken  
 9 by Terpin *after* the January 2018 SIM Swap that it contends contributed to the theft.  
 10 Indeed, the only *actions* that occurred *after* the January 2018 SIM Swap were that  
 11 Pinsky and the other perpetrators did exactly what they had set out to do (and which  
 12 AT&T had predicted and which Pinsky had done previously to others), i.e.,  
 13 accessing accounts by resetting passwords and searching and locating and stealing  
 14 the victim's "financial accounts" (in the form of cryptocurrency).<sup>6</sup>

---

16  
 17       <sup>5</sup> *Modisette v. Apple Inc.*, 30 Cal.App.5th 136 (2018), likewise involved a plaintiff  
 18 with no connection to the defendant, Apple. Guided in part on policy  
 19 considerations about the potential limits on of liability to third parties, the court  
 20 found that Apple had no duty to those third parties. By contrast, AT&T clearly  
 21 owed duties to Terpin to protect his account by requiring reasonable authentication  
 22 procedures to protect his communications and identifying and investigating bad  
 23 actor employees such as Smith. Similarly, the *Modisette* court concluded that the  
 24 driver, not Apple, was the cause of the injury, and that a reasonable person would  
 not consider Apple a cause of the accident. *Id.* In contrast, the actions of those  
 who caused Terpin harm were foreseeable, as shown in AT&T's September 27,  
 2017 Cyber Aware Blog referencing precisely such actions by a "thief" and  
 Pinsky's testimony that the cryptocurrency theft was what he hoped to achieve.  
 (See also Order on Motion to Dismiss, Dkt. 37 at 5-7). As Pinsky had no other way  
 to access and steal from Terpin's accounts without the unauthorized SIM swap, the  
 SIM swap was not only a but for cause but a critical and necessary step to achieving  
 the theft.

25       <sup>6</sup> While AT&T may attempt to base a comparative fault defense on Terpin's  
 26 security practices, AT&T cannot circumvent long settled California law that  
 27 contributory fault is not a complete bar to plaintiff's recovery, *Li v. Yellow Cab Co.*,  
 28 13 Cal.3d 804 (1975). Should his security practices be raised as part of a  
 comparative fault defense, Terpin has every expectation that the jury will find  
 AT&T primarily, if not entirely, responsible for the resulting injury.

## V. CONCLUSION

For the reasons set forth above, the Court should deny AT&T's motion for summary judgment.

Dated: February 6, 2023

*F. C. Danner*

By:

PIERCE O'DONNELL (SBN 081298)  
TIMOTHY J. TOOHEY (SBN  
140117)  
PAUL BLECHNER (159514)  
Attorneys for Plaintiff Michael Terpin

**GREENBERG GLUSKER FIELDS CLAMAN  
& MACHTINGER LLP**  
2049 Century Park East, Suite 2600  
Los Angeles, California 90067

## **LOCAL RULE 11-6.2 Certificate of Compliance**

The undersigned, counsel of record for Plaintiff Michael Terpin, certifies that this brief contains 6,613 words, which complies with the word limit of L.R. 11-6.1

Dated: February 6, 2023

By: /s/ Timothy J. Toohey

PIERCE O'DONNELL (SBN 081298)  
TIMOTHY J. TOOHEY (SBN 140117)  
PAUL BLECHNER (159514)  
Attorneys for Plaintiff Michael Terpin

Attorneys for Plaintiff Micha l Terpin

**GREENBERG GLUSKER FIELDS CLAMAN  
& MACHTINGER LLP**  
2049 Century Park East, Suite 2600  
Los Angeles, California 90067